13 August 1985

25X1 MEMORANDUM FOR: [redacted]
SECOM

25X1 FROM: [redacted] (C)
Deputy Chief, Special Security Center

SUBJECT: SECOM Agenda Item for 21 August 1985, Co-utilization of Sensitive Compartmented Information Facilities (SCIFs)

REFERENCES: A. Memo fr C/ISG to C/PPG dtd 25 July 1985
B. Meeting/Discussions 6 August 1985

It has been agreed that in any modification of DCID 1/19 or it equivalent, the SECOM publication entitled "Security Policy Manual for SCI Control Systems," it is necessary to include some wording relative to Co-utilization of SCIFs. The following is offered as a draft recommendation for inclusion in the Policy Manual for SCI Control Systems. Specifically, the proposed text is recommended for placement on page 5, following "13. Accreditation of SCIFs."

"14. Co-utilization of SCIFs. In the interest of efficient use of resources and perpetuation of cooperation between agencies of the Community, co-utilization of industrial contractor SCIFs is encouraged. The mechanism for establishing such co-utilization is the Memorandum of Agreement (MOA).

a. A MOA is an agreement in which a Cognizant Security Authority (CSA) permits another agency joint use of an industrial contractor SCIF. A MOA is required whenever one agency will utilize a contractor SCIF already under the security cognizance of another agency. A generally acceptable example format for documenting such an agreement is found in Defense Intelligence Agency Manual (DIAM) 50-5, Volume I. However, certain additional elements required are:

25X1

1. Type of material to be used, processed or stored within the SCIF. (e.g. SI, TK, etc.)

2. Type of storage required (open or closed).

3. Anticipated volume of material (in terms of security containers).

4. Duration for which the co-utilization is requested.

An optional but not mandatory element would be the contract(s) number(s) relative to the efforts on behalf of the requesting agency.

b. If a formal MOA is utilized, the requesting agency is responsible for originating the document. Signatories at a minimum, must be responsible officials of the CSA, the requesting user agency and the contractor. Some MOA's must be classified in deference to covert relationships existing between certain agencies and contractors. Originators of MOA's are responsible for determining if classification (and the level) is required.

c. Formal MOA's, by nature of the requirement for several signatories, are time consuming. In lieu of the formal MOA, exchange of electrical messages between CSAs and requesting agencies is permissible, provided they contain all appropriate elements and are approved by appropriate officials. A statement to the effect that standard MOA conditions will apply infers that the conditions in the DIAM 50-5 example will be followed. The hard copies of the message exchange will then constitute documentation for the MOA.

d. If a user agency desires the contractor to make any substantive changes in procedures or physical characteristics of a SCIF, the proposed changes must have the concurrence of the CSA

e. It is imperative that the user agency notify the CSA when the co-utilization is no longer required.

f. Co-utilization of computer systems at contractor facilities is a more complex issue. A MOA for co-utilization of a contractor SCIF does not

automatically include approval for joint use of computer systems with that SCIF. A separate MOA is required for co-utilizition of computer systems. The system itself must be certified by a CSA as meeting the appropriate computer security standards. The system can only be operational if within an accredited SCIF. A MOA for joint use of a computer system is mandatory when two or more agencies are simultaneously processing SCI on the same system. A MOA may not be required only because multiple agencies make use of the same system. Different criteria are used to determine the CSA over a particular system, e.g. highest percentage of use of the system; cognizance over the physical SCIF etc. Formal, written documentation to effect a MOA for computer systems is required although interim agreements for joint use may be enacted through electrical message exchange. DCID 1/16 contains additional information concerning joint use of computer systems. (U)

25X1

(C)

prescribed in NFIB/NFIC-9.1/47, "U.S. Intelligence Community Physical Security Standards for SCI Facilities," effective 23 April 1981, or successor policy statements.

13. **Accreditation of SCIFs.** The DCI shall accredit all SCIFs except where that authority has been specifically delegated or otherwise provided for. The CIA Office of Security shall accredit SCIFs for Executive Branch departments and agencies outside the Intelligence Community and for the Legislative and Judicial Branches. The accreditation shall state the category(ies) of SCI authorized to be stored/processed in the SCIF. Accrediting officials shall maintain a physical security profile on each of their SCIFs to include data on any waivers of standards.

14. **Emergency Plans.** Each accredited SCIF shall establish and maintain an approved emergency plan. This may be part of an overall department, agency, or installation plan, so long as it satisfactorily addresses the considerations stated below. Emergency planning shall also take account of fire, natural disasters, entrance of emergency personnel (e.g., host country police and firemen) into a SCIF, and the physical protection of those working in such SCIFs. Planning should address the adequacy of protection and firefighting equipment, of evacuation plans for persons and SCI, and of life-support equipment (e.g., oxygen and masks) that might be required for personnel trapped in vault-type SCIFs.

a. In areas where political instability, host country attitude, or criminal activity suggests the possibility that a SCIF might be overrun by outsiders, emergency plans must provide for the secure destruction/removal of SCI under adverse circumstances, to include such eventualities as loss of electrical power, nonavailability of open spaces for burning or chemical decomposition of material, and immediate action to be taken if faced with mob attack. Where the risk of overrun is significant, holdings of SCI must be reduced to, and kept at, an absolute minimum needed for current working purposes, with reference or background material to be obtained, when needed, from other activities and to be returned or destroyed when it has served its purpose.

b. Emergency plans shall be reviewed annually and updated as necessary. All personnel shall be familiar with the plans. In areas where political or criminal activity suggests the possibility that the SCIF might be overrun by outsiders, drills shall be conducted as local circumstances warrant but no less frequently than annually to ensure testing and adequacy of plans.

15. **Two-Person Rule.** NFIB/NFIC-9.1/47 establishes policy on this subject, which is quoted below for ready reference:

> "As a matter of policy, SCI Control Facilities (SCIFs) should be staffed with sufficient people to deter unauthorized copying or illegal removal of SCI. SCIF designated communication centers, document control centers (registries), and like facilities that handle or store quantities of SCI must be manned while in operation by at least two appropriately indoctrinated persons in such proximity to one another as to provide mutual support in maintaining the integrity of the facility and the material stored therein. The granting by an SOIC of exceptions to this policy will be made a matter of record and should involve consideration of the proven reliability and maturity of the persons involved; the volume, variety, and sensitivity of the holdings in the facility; and whether or not the persons involved are subject to periodic polygraph examinations as a condition of access. Exceptions for communications centers, document control centers, and the like should be granted in only extraordinary